# Department of Homeland Security
# Information Analysis and Infrastructure Protection
# Daily Open Source Infrastructure Report for 23 March 2004

Current Nationwide Threat Level is
ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS
For info click here
www.whitehouse.gov/homeland

**Daily Overview**

- Reuters reports the government has arrested a Texas man who crafted fake e−mail messages to trick hundreds of America Online and Paypal users into providing credit card numbers and other sensitive information. (See item 5)
- Newsday reports some senators and members of Congress are warning that Pennsylvania Station and other U.S. rail facilities are vulnerable to an attack similar to that in Madrid, Spain. (See item 10)
- Food Safety Inspection Service reports the U.S. Department of Agriculture's Food Safety and Inspection Service has announced that Plumrose USA, Inc, of Booneville, MS, is voluntarily recalling approximately 94,800 pounds of roast beef because of undeclared allergens of wheat and soy protein. (See item 14)
- Security Focus has raised ThreatCon to Level 2, citing the need for increased vigilance. Please refer to the Internet Alert Dashboard.

**DHS/IAIP Update *Fast Jump***

**Production Industries:** Energy; Chemical; Defense Industrial Base
**Service Industries:** Banking and Finance; Transportation; Postal and Shipping
**Sustenance and Health:** Agriculture; Food; Water; Public Health
**Federal and State:** Government; Emergency Services
**IT and Cyber:** Information and Telecommunications; Internet Alert Dashboard
**Other:** General; DHS/IAIP Web Information

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

**1.**

*March 22, Reuters* — **Europe ready to meet tough U.S. gasoline specs, at a price. Some of Europe's biggest hitters in the gasoline export trade say they can supply the United States with high specification summer fuel, meeting stringent new U.S. regulations, but warn hefty price premiums would be needed to make such flows profitable.** This will go some way to allay fears that bans by New York state, Connecticut and California on gasoline blending component methyl tertiary butyl ether, (MTBE) coupled with a U.S.−wide cut in sulphur limits in gasoline, could result in shortages in the peak driving season from late May to early September. However, assessments by oil majors and export−oriented refiners will add to worries that U.S. motorists, already hit by pump prices near record highs, will face yet higher fuel costs, especially those living in states that have this year outlawed MTBE. **New York and Connecticut rely on imports for 60 percent of their gasoline supply. Europe supplies about a quarter of total U.S. import requirements, with the bulk of transatlantic flows landing in New York harbor.** The two states account for roughly a third of the U.S. east coast's 1.235 million bpd consumption of reformulated gasoline. California accounts for the bulk of west coast total gasoline consumption of 1.1 million bpd.
Source: http://biz.yahoo.com/rm/040322/energy_gasoline_survey_2.html

[Return to top]

## Chemical Sector

2. *March 22, Dubbo Daily Liberal (Australia)* — **Nuclear fears raised by spill. A chemical semi−trailer crash on Thursday, March 18, highlighted the risk of trucking nuclear waste through Dubbo (Australia) and other western towns,** State MP Tony McGrane said yesterday, March 21. The Dubbo accident and a recent fatal chemical spill in the Blue Mountains were perfect examples of what could go wrong, he said. McGrane was a member of a cross−party committee that last month recommended opposing the transport of nuclear waste through NSW. He said the Federal Government needed to do a lot more homework before it could convince people of the safety of transporting nuclear waste. "The committee found there are massive problems with the back−up safeguards in existence now. A lot more research and consultation needs to be done − these incidents highlight the fact we've got to be more careful before proposing anything. District emergency management officer Stuart Davies said the initial response to a nuclear waste incident would be similar to that for Thursday's accident. "A containment area would be set up until specialist resources could come up to Dubbo," he said.
Source: http://dubbo.yourguide.com.au/detail.asp?class=news&subclass=local&category=general news&story_id=294198&y=2004&m=3−

[Return to top]

## Defense Industrial Base Sector

3. *March 22, Wired News* — **Better bombing through technology.** The media covering U.S. military campaigns in Afghanistan and Iraq called them "bunker busters" −− bombs that were designed to dig deep into the ground before detonating. Now, **the Pentagon is attempting to refine the way targets are identified before using these smart bombs through something called the Counter Underground Facilities (CUGF), program. Under the auspices of the**

**Defense Advanced Research Projects Agency's Special Projects Office, CUGF researchers are working to develop technologies intended to pinpoint the location, size and mission of underground facilities, determine the pace at which the mission is being carried out, recommend the optimum time for a pre−emptive strike, and monitor the results of that strike.** Data from the sensors −− which will be implanted near suspected underground installations or configured as a Low−Altitude Airborne Sensor System carried by a small unmanned aircraft −− will be uploaded to an intelligence−gathering airplane. Once acquired and verified, data from each sensor will be analyzed to extract basic information. Software using sophisticated proprietary algorithms will take the raw data from the sensors, along with the information developed from individual analysis of that data and use it all to generate an analytical report.
Source: http://www.wired.com/news/technology/0,1282,62704,00.html

4. *March 19, Air Force Press News* — **AWACS voice recognition may enhance accuracy.** The Airborne Warning and Control System (AWACS) program office is developing software that could eliminate the mouse on the E−3 Sentry. Voice−recognition software allows an air battle manager to control his or her radar screen by speaking to it, instead of using a traditional trackball or mouse, keyboard and function keys. "We estimate that, by adding a robust speech−recognition capability to the E−3 weapon system, the operator is able to reduce his or her workload by up to 40 percent, improve accuracy and increase overall situational awareness," said 1st Lt. Jeff LaFleur, AWACS advanced technology program manager. "While the program is just getting started, **the outstanding potential to provide increased situational awareness for air battle managers has generated strong interest from the AWACS community and could pave the way for … other platforms to be voice−enabled in the future," said Col. Brian Waechter,** AWACS Materiel Wing director.
Source: http://www.af.mil/news/story.asp?storyID=123007252

[Return to top]

## Banking and Finance Sector

5. *March 22, Reuters* — **U.S. shuts down 'phishing' scam. The U.S. government said on Monday, March 22, it had arrested a Texas man who crafted fake e−mail messages to trick hundreds of Internet users into providing credit card numbers and other sensitive information. Zachary Hill of Houston pleaded guilty to charges related to a "phishing" operation,** in which he sent false e−mails purportedly from online businesses to collect sensitive personal information from consumers, the Federal Trade Commission (FTC) said. According to the FTC, **Hill sent out official−looking e−mail notices warning America Online and Paypal users to update their accounts to avoid cancellation.** Those who clicked on a link in the message were directed to a Website Hill set up that asked for Social Security numbers, mothers' maiden names, bank account numbers and other sensitive information, the FTC said. Hill used the information he collected to set up credit−card accounts and change information on existing accounts, the FTC said. He duped 400 users out of at least $75,000 before his operation was shut down on December 4, FTC attorneys said.
Source: http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=4624987&section=news

6. *March 21, UPI* — **Bank information tape missing in Singapore. A magnetic tape containing information on 123,690 customer accounts at Citibank's Japan unit has reportedly been missing since February 21 from Singapore.** The tape disappeared while it was being transported by a security company in Singapore to a data−processing center that manages customer information for Japan and other Asian economies. **The tape had backup information of monthly bank statements, including customers' names, addresses, account numbers and account balances, however personal identification numbers were not included.** Citibank said the tape does not contain information that a third party could use to withdraw cash from accounts −− and that only a special computer system could read the information.
Source: http://washingtontimes.com/upi−breaking/20040321−105658−6419 r.htm

7. *March 21, electricnews.net* — **Phatbot primed to steal your credit card details. A Trojan horse−type computer virus called Phatbot can steal credit card numbers and launch denial of service attacks on Websites.** The new virus made its debut on the Internet on Friday, March 18, clogging bandwidth, stealing personal data and initiating denial of service attacks. Phatbot is a variant of a Agobot, a big family of IRC bots. **It can steal personal information such as e−mail addresses, credit card numbers, PayPay details and software licensing codes. It forwards this information using a peer−to−peer (P2P) network, rather than IRC channels exploited by its predecessors.** Phatbot can also kill any anti−intrusion devices and give people a false sense of security in order to get inside a network and exploit vulnerabilities, Internet security company F−Secure says. So far, Phatbot infections are limited and some e−security companies are still rating it low−to−medium risk, said Conor Flynn, technical director of U.S. e−security company Rits.
Source: http://www.theregister.co.uk/content/6/36414.html

8. *March 19, SecurityFocus* — **Phishing attacks on the rise according to report. February saw a marked increase in the number of new variations of the spam−borne swindle called "phishing," according to a report from the Anti−Phishing Working Group released Friday, March 19. The group charted 282 unique attacks last month, a 60 percent increase above the 176 attacks spotting in January.** "The number of attacks is growing, and the rate of increase is growing," says Dan Maier, director of marketing for the group. As in months past, eBay was the most commonly−spoofed company in the February line−up, with 104 different scam messages in circulation. Citibank and PayPal were a distant second and third place with 58 and 42 respectively. Overall, the swindlers appear to be using a wider variety of scammy mailings, but are drawing on a smaller pool of brands, says Maier. In February, **the phishers exhibited increased sophistication in constructing Web pages that obfuscate the path that the purloined information takes to get back to the scammers** −− the easiest route to tracking them down. "If you look at the code, the people doing this are getting much better at disguising where the information is going," says Maier.
Source: http://www.securityfocus.com/news/8289

[Return to top]

# Transportation Sector

9.

*March 23, Department of Transportation* — **U.S. Transportation Secretary Mineta announces $27.3 million in grants to expand capacity, enhance safety at Alaska airports.** U.S. Transportation Secretary Norman Y. Mineta today announced $27.3 million in grants to expand capacity and enhance safety at airports in Alaska, an action that will provide economic benefits to the communities receiving the funds. The grants will go to Ted Stevens Anchorage International Airport and Sand Point Airport. Ted Stevens Anchorage International Airport will receive a total of $18.4 million. A grant of $7 million will help reduce the impact of airport noise on communities surrounding the airport. A total of $6.4 million will be used to construct a taxiway and widen a runway. A grant of $5 million will be used to rehabilitate a runway and for apron construction, expansion and rehabilitation. **The funds come from the Airport Improvement Program of the U.S. Department of Transportation's Federal Aviation Administration.**
Source: http://www.dot.gov/affairs/dot3404.htm

10. *March 22, Newsday* — **Terror concerns: A danger on the trains.** Some Northeastern senators and members of Congress are warning that Pennsylvania Station and other U.S. rail facilities are vulnerable to a similar attack to that in Madrid, Spain. **More train security measures and funding are needed, they say, to protect the U.S. railways.** Sen. John McCain (R−AZ) plans a hearing tomorrow, March 23, to address what additional steps should be taken in the wake of the Spanish train bombing to protect the American rail system from attack, according to a committee official. **In Penn Station alone − the busiest railroad station in the United States with 21 tracks and 15 miles of tunnels −− 750 trains and 500,000 commuters pass through every weekday,** according to Department of Transportation Inspector General Kenneth Mead. This year, there are renewed efforts to increase railroad security, including an $898−million bill by Rep. Peter King (R−Seaford) to heighten security in Penn Station tunnels as well as tunnels in the Baltimore/Washington area.
Source: http://www.newsday.com/news/nationworld/nation/ny−ustran2237 18275mar22,0,1635089.story?coll=ny−nationalnews−headlines

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

11. *March 22, USAgNet* — **South Korea confirms new case of bird flu.** South Korea's agriculture ministry confirmed on Monday, March 22, the first case of bird flu in the country for more than one month. **The outbreak uncovered at the weekend at a chicken farm in Kyonggi province was the first case since February 5 and 16,000 poultry were destroyed on Sunday**, a ministry official said. A further 400,000 poultry in the affected area north of Seoul would also be destroyed, the official added. More than 20 people across Asia have died as a result of bird flu, which can in the case of certain strains be fatal for humans, although South Korea has had no human fatalities. So far nearly five million poultry have been destroyed in

South Korea since an outbreak of the disease late last year.
Source: http://www.usagnet.com/story−national.cfm?Id=298&yr=2004

[Return to top]

## Food Sector

12. *March 22, Baltimore Sun* — **Threat to food supply on rise. The potential threat to our food increases as the world's population grows, travels more, harvests more of the world's forests and relies increasingly on crops supplied by industrial−size farms, experts say. "I think what we're seeing is an unprecedented vulnerability of the safety of our food supply," said Dr. Robert Lawrence,** a professor of preventive medicine at the Johns Hopkins University's Bloomberg School of Public Health. Experts say the threat is a direct result of our own appetites. "It's very much related to what the American consumer is looking for, the desire for seasonal fruit and vegetables year−round," said Dr. David W.K. Acheson, director of food safety and security for the Food and Drug Administration (FDA). In an attempt to monitor the flood of imports, the FDA has hired 600 inspectors and plans to require 420,000 food importers to register and notify the agency before shipping food into the U.S. Under new regulations, importers must give two hours' notice for goods moved by truck, four hours' notice for rail shipments and eight hours for ships coming into ports. The regulations are intended to make it easier for FDA inspectors to identify incoming foodstuffs that might be suspicious.
Source: http://www.baltimoresun.com/news/health/bal−te.pathogens22mar22,0,3143619.story?coll=bal−home−headlines

13. *March 22, Wisconsin Ag Connection* — **Edy's recalling mislabeled ice cream. Edy's Grand Ice Cream is recalling 14,000 cartons of ice cream in 25 states that may contain peanuts not listed on the label. The ice cream was distributed in the Midwest, Mid−Atlantic and Northeast, the company said. The affected Toffee Bar Crunch ice cream and Peanut Butter Cup ice cream have the code 18−1644 11 27 6B or 18−1644 11 27 6D printed on the bottom of the carton.** The company said a small number of the 1.75−quart cartons may be mislabeled −− some cartons feature Toffee Bar Crunch with carton lids featuring Peanut Butter Cup −− and the ice cream may include peanuts, not declared on the label. People who have an allergy or severe sensitivity to peanuts may run the risk of serious or potentially life−threatening allergic reaction if they consume this product. No allergic reactions have been reported.
Source: http://www.wisconsinagconnection.com/story−state.cfm?Id=356& yr=2004

14. *March 19, Food Safety Inspection Service* — **Mississippi firm recalls roast beef because of undeclared allergens.** Plumrose USA, Inc, a Booneville, MS, firm is voluntarily recalling approximately 94,800 pounds of roast beef because of undeclared allergens (wheat and soy protein), the U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) announced Friday, March 19. **The products being recalled are 1) Schlotzsky's Deli, sliced & fully cooked, roast beef in 8 oz. vacuum sealed packages; 2) Schlotzsky's Deli, sliced & fully cooked, choice angus roast beef in 14 oz. vacuum sealed packages; and 3) Danola Supreme, Angus Roast Beef in 8 oz. vacuum sealed packages.** All of the packages bear the establishment number "EST. 26A" inside the USDA mark of inspection. The products were produced between October 1, 2003 and March 12, 2004. They were distributed to retail

stores in California and Oregon. Consumers who are allergic to wheat or soy protein should not eat this product, but return it to the point of purchase. FSIS has received no reports of allergic reactions associated with consumption of this product. The problem was discovered by FSIS.
Source: http://www.fsis.usda.gov/OA/recalls/prelease/pr009−2004.htm

[Return to top]

## Water Sector

15. *March 22, Water Tech Online* — **Rural water supplies at risk in Ohio. The Ohio Environmental Protection Agency has been testing drinking wells in Clark County since receiving an alarming number of reports of murky water, starting in the late 1990s. Signs of bacterial contamination turned up in about one−third of the wells examined. The study by geologist Rich Bendula and biologist Bob Moore of the Ohio EPA points to potential risks faced by people who get their drinking water from rural private wells or small public water supplies, the paper reported.** The dangers are particularly acute after heavy spring rains, which can flush contaminated surface water into wells through cracks and fissures in the underground bedrock, the article stated. Potential hazards are greater in rural water supplies, which are infrequently tested. The report concludes that wells that are commonly dug to a shallow depth, encountering bedrock at four to six feet, were at the highest risk of being contaminated with bacteria. The depth of the well casings and grouting around the casings are also important factors, the paper reported. In contrast, wells dug to depths of 18 to 22 feet only showed periodic contamination with coliform bacteria.
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=46662

16. *March 22, Water Tech Online* — **Water bond stirs controversy.** The chance that water project funds could go to California's for−profit companies is causing some unrest. **Representatives of public water agencies say that the plan to allow private water utilities to apply for grants and loans from the $3.4 billion water bond should be abandoned because voters never knew the money could go to private companies.** At issue are guidelines being developed at three state agencies for applying for funding under Proposition 50. One of those agencies, the Department of Health Services, says it plans to allow private water companies access to funding for infrastructure improvements. The department has authority over $435 million from the bond to improve drinking water quality and another $50 million for security. **Roughly 20 percent of Californians get their drinking water from private companies, according to Susan Conway, president of the California Water Association, which represents private water companies.**
Source: http://www.watertechonline.com/news.asp?mode=4&N_ID=46670

[Return to top]

## Public Health Sector

17. *March 22, U.S. Newswire* — **New initiative will improve bioterrorism preparedness of health workforce. Congress has asked the nation's bioterrorism experts to target new mechanisms to increase the level of preparedness for the health workforce. Vaccines,**

**drugs, diagnostic devices and medical surveillance are all crucial tools in the fight against bioterrorism and emerging infectious disease, but experts say these are not enough.** Until now, preparedness efforts have focused primarily on material solutions such as protective gear and information analysis; there has been much less emphasis on training the health workforce who will use this equipment. Now the Association of Academic Health Centers (AHC) will collaborate with Michael Hopmeier, a counterterrorism expert, to operate the Healthcare Incentivization Working Group (HIWG), which will work with academic health centers and public health systems to defray the tremendous costs of preparedness training for the workforce. Joining HIWG in this effort is the National Center for Emergency Preparedness, housed at Nashville's Vanderbilt University Medical Center, an AHC member institution.
Source: http://releases.usnewswire.com/GetRelease.asp?id=140−0322200 4

[Return to top]

## Government Sector

18. *March 22, Federal Computer Week* — **CIO Council to consider smart card rule. A proposed policy requiring all federal agencies to use smart cards for employee IDs is awaiting approval by the CIO Council after being adopted by the Federal Identity and Credentialing Committee. General Services Administration officials said the policy would become official if the Office of Management and Budget issues it after action by the CIO Council. They described it as a major milestone in the development of a governmentwide identification system.** GSA coordinates the work of the committee, an interagency group that works with the CIO Council and the E−Authentication team at OMB. The draft policy has no deadlines for agency action, but it states that "agencies should begin planning for migrating their current access control systems, both physical and logical, in order to conform to this policy." The policy calls for agencies to adopt standards that will make the cards interoperable across the federal government's sensitive but unclassified networks. That way, a federal employee or contractor visiting another agency's offices could simply wave his or her card at the reader and be recognized.
Source: http://www.fcw.com/fcw/articles/2004/0315/web−smart−03−19−04 .asp

[Return to top]

## Emergency Services Sector

19. *March 22, Reuters* — **Australia stages mock terror attack. Australia has embarked on its largest counter−terrorism exercise, staging a mock bomb attack on the prime minister's car and an oil rig takeover as the government plans a review to boost security at ports.** Police, defense and intelligence officials from four of Australia's eight states and territories were taking part in the five−day exercise which involves responding to various crises and testing new chemical, biological and radiological equipment. Attorney−General Philip Ruddock said the exercise, codenamed 'Mercury '04' and 18 months in the planning, would test the ability of national agencies to communicate with each other and respond to long−distance terror incidents.'You've got to test various scenarios, people have to be able to demonstrate they have the skills, the capacity, the equipment to be able to deal with potentially real life situations,'

Ruddock told reporters after touring Mercury '04 headquarters.
Source: http://www.reuters.co.uk/newsPackageArticle.jhtml?type=worldNews&storyID=480408&section=news

20. *March 22, Associated Press* — **Florida proposes additional $75 million for domestic security.** The Florida House has proposed spending an extra $75 million on the state's security infrastructure next year, with the largest portion going to fix up National Guard armories. If the proposal goes through, it would mark the first time the state spent money that wasn't matched by the federal government on homeland security needs, said Rep. Bruce Kyle, R−Fort Myers, chairman of the House Appropriations Committee. The proposal would send $35 million to repair armories. Half of Florida's 58 armories are more than 40 years old, said Maj. Gen. Douglas Burnett, commander of the Florida National Guard. **Another $15 million would be earmarked for port security patrols and access controls. Other portions of the money would go toward communications improvements, anti−terrorism training for first responders and better coordination among departments.** By spending $1.5 million for law enforcement data sharing, officials are hopeful all the state's 355 police agencies could be tied together over the next two to three years. Already, 45 agencies along the Interstate 4 corridor are linked to share information, said Orange County Sheriff Kevin Beary.
Source: http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/2004 0322/APN/403220777

21. *March 22, USA TODAY* — **Security focus stays on planes, bioterror. Homeland Security Secretary Tom Ridge is expected to announce several new rail−security programs today to address a growing demand for security upgrades following the terrorist bombings in Madrid this month. But U.S. officials say most of their money and attention will remain on aviation security and bioterrorism.** Administration officials said Sunday that Ridge will announce several small−scale efforts to tighten rail security. The department will create a "rapid−deployment mass transit program," including teams with explosives−sniffing dogs that can be sent to vulnerable rail systems and stations when intelligence suggests a threat. The department also will speed up plans for a pilot program to test whether explosives−detection technology can be used to screen rail passengers and bags. The technology will be tested at a commuter rail station. **But despite the Madrid bombings, which killed 202 people and wounded more than 1,800, officials say they must focus on the kinds of attacks that could do the most damage.** A bioterrorism attack that could kill hundreds of thousands of people with smallpox or another deadly agent is by far the most serious concern facing Homeland Security officials.
Source: http://www.usatoday.com/news/washington/2004−03−21−security− plans_x.htm

[Return to top]

## Information and Telecommunications Sector

22. *March 22, eWEEK* — **Netsky.P spreads through ancient security hole.** A new variant of the Netsky worm, Netsky.P, is spreading quickly. This new variant is very much like other Netsky versions with two differences, according to Vincent Gullotto of the McAfee Avert Virus and Vulnerability Emergency Response Team. **The initial seating of the worm, referring to the initial group of users to whom the virus author distributed it, appears to have been in Australia**. It's not clear whether or how this would facilitate spreading of the worm, but it is

unusual. The other unusual characteristic of this worm is that **it utilizes a very old vulnerability in Internet Explorer, the Incorrect MIME Header (MS01−020) bug**. This bug, patched almost three years ago, allowed a hostile HTML e−mail to execute arbitrary code if viewed in the preview pane of a mail client. Like other Netsky variants, this one spreads mainly through a built−in SMTP engine to e−mail addresses harvested out of the user's files.
Source: http://www.eweek.com/article2/0,1759,1552315,00.asp

### Internet Alert Dashboard

**Current Alert Levels**

| | |
|---|---|
| AlertCon: 2 out of 4<br>https://gtoc.iss.net | Security Focus ThreatCon: 2 out of 4<br>http://analyzer.securityfocus.com/ |

**Current Virus and Port Attacks**

| | |
|---|---|
| **Virus:** | #1 Virus in the United States: **WORM_LOVGATE.G**<br>Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center<br>[Infected Computers, North America, Past 24 hours, #1 in United States] |
| **Top 10 Target Ports** | 445 (microsoft−ds), 135 (epmap), 80 (www), 3127 (mydoom), 25 (smtp), 137 (netbios−ns), 1433 (ms−sql−s), 1434 (ms−sql−m), 139 (netbios−ssn), 4899 (radmin)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

[Return to top]

## General Sector

**23.** *March 21, New Scientist* — **Experts fear terrorists are seeking fuel−air bombs.** Some experts fear that terrorists are trying to develop thermobaric and fuel−air bombs. The devices use a small charge to generate a cloud of explosive mixed with air. The main explosion is then detonated by a second charge (a fuel−air explosion), or by the explosive reacting spontaneously with air (a thermobaric explosion). **The resulting shock wave is not as strong as a conventional blast, but it can do more damage as it is more sustained and, crucially, diminishes far more gradually with distance**. In 2002 a tanker truck was used in a suicide attack on a synagogue in Tunisia, thought to be the work of al Qaeda. Some experts think the way the fuel tanks were rigged with explosives shows a knowledge of fuel−air explosive techniques. The Canadian defence research and development agency DRDC is taking the threat so seriously that it is testing thermobaric devices itself in an attempt to develop defenses against them. And **the U.S. Marine Corps is using computerized war games to devise tactics that could help minimize casualties if insurgents in countries such as Iraq use thermobaric weapons in attacks.**
Source: http://www.newscientist.com/news/news.jsp?id=ns99994785

[Return to top]

## DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

### DHS/IAIP Daily Open Source Infrastructure Report Contact Information

| | |
|---|---|
| Content and Suggestions: | nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 |
| Subscription and Distribution Information | Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information. |

### Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at info@us−cert.gov or visit their Web page at www.uscert.gov.

### DHS/IAIP Disclaimer